

17 MAG 4291

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All  
Content and Other Information  
Associated with Four Email Accounts,  
Two Dropbox Accounts, Two Twitter  
Accounts, and Three Instagram  
Accounts

USAO Reference No. 2017R00116.

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

**Agent Affidavit in Support of Application for Search Warrants  
for Stored Electronic Communications**

STATE OF NEW YORK     )  
                                  ) ss.  
COUNTY OF NEW YORK    )

JOSEPH T. COSTELLO, being duly sworn, deposes and states:

**I. Introduction**

**A. Affiant**

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for approximately three years. Prior to joining the FBI, I served as a Special Agent with the U.S. Department of State, Diplomatic Security Service, for approximately five years. For the last approximately two years, I have been assigned to the FBI's New York Joint Terrorism Task Force ("JTTF"). During this time period, I have participated in numerous investigations of unlawful activity, principally national security related matters and crimes relating to immigration fraud. During the course of these investigations, I have conducted or participated in surveillance, the introduction and debriefings of informants, and the execution of search warrants. Through my training, education, and experience, I have become familiar with various terrorist organizations, as well as the manner in which terrorists are recruited, receive training, and operate, and some of the methods that are used to conceal evidence of participation in such illegal activity. I have received

training in the use of computer technology by terrorist networks and have participated in investigations involving the use of computers, the Internet, and social media by terrorists and terrorist organizations. Through my training and experience, I have become familiar with some of the ways in which terrorists and terrorist groups use the Internet, including social media and email, to promote their activities, recruit new members, and issue threats, and I have also participated in the execution of search warrants involving electronic evidence.

**B. The Providers, the Subject Accounts and the Subject Offenses**

2. I make this affidavit in support of an application for search warrants pursuant to Title 18, United States Code, Section 2703, for all content and other information associated with the following "Subject Accounts":

a. The email account holy.smoke.shop.franklin@gmail.com, which is maintained and controlled by Google, Inc. ("Google"), headquartered in Mountain View, California;

b. The email account jacob.kouran@gmail.com, which is maintained and controlled by Google;

c. The email account wmc.sportswear@gmail.com, which is maintained and controlled by Google;

d. The email account jacobfashion@hotmail.com, which is maintained and controlled by Microsoft Corporation ("Microsoft"), headquartered in Redmond, Washington;

e. The Dropbox account associated with the email address ali.m.kourani@gmail.com, which is maintained and controlled by Dropbox, Inc. ("Dropbox"), headquartered in San Francisco, California;

f. The Dropbox account associated with email address alikuku@hotmail.com, which is maintained and controlled by Dropbox;

g. The Twitter account associated with the email address ali.m.kourani@gmail.com, which is maintained and controlled by Twitter, Inc. (“Twitter”), headquartered in San Francisco, California;

h. The Twitter account associated with the email address alikuku@hotmail.com, which is maintained and controlled by Twitter;

i. The Instagram account associated with the email address ali.m.kourani@gmail.com, which is maintained at premises controlled by Facebook, Inc. (“Facebook”) and Instagram LLC (“Instagram”), headquartered in Menlo Park and San Francisco, California;<sup>1</sup>

j. The Instagram account associated with the email address alikuku@hotmail.com, which is maintained at premises controlled by Facebook and Instagram; and

k. The Instagram account associated with the email address jacob.kouran@gmail.com, which is maintained at premises controlled by Facebook and Instagram.

3. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrants.

4. As detailed below, there is probable cause to believe that the Subject Accounts contain evidence, fruits, and instrumentalities of violations of: (i) Title 18, United States Code, Section 2339B (providing, attempting to provide, and conspiring to provide material support or resources to a designated foreign terrorist organizations (“FTO”)); (ii) Title 18, United States Code, Sections 2339D and 371 (receipt of, and attempting and conspiring to receive, military-type training from

---

<sup>1</sup> Google, Microsoft, Dropbox, Twitter, Instagram, and Facebook are referred to herein as the “Providers.”

an FTO); (iii) Title 18, United States Code, Section 924 (firearms offenses related to crimes of violence); (iv) Title 50, United States Code, Section 1705 (making or receiving a contribution of funds, goods, and services to and from a specially designated terrorist); (v) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (vi) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the “Subject Offenses”). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

### **C. Services and Records of Microsoft and Google**

5. I have learned the following about Microsoft and Google:

a. The Microsoft and Google offer email services to the public. In particular, Microsoft and Google allow subscribers to maintain email accounts under domain names such as gmail.com or Hotmail.com. A subscriber using these Providers’ services can access his or her email account from any computer connected to the Internet.

b. Microsoft and Google maintain the following records and information with respect to every subscriber account:

i. *Email Contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber’s account, or stored in draft form

in the account, is maintained on servers of Microsoft or Google unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on the computers of Microsoft or Google indefinitely. Even if the subscriber deletes the email, it may continue to be available on the servers of Microsoft or Google for a certain period of time.

ii. *Address Book.* Microsoft and Google also allow subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and Billing Information.* Microsoft and Google collect and maintain (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Microsoft and Google also maintain records concerning the date on which the account was created, the Internet protocol (“IP”) address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Microsoft and Google maintain records of the subscriber’s means and source of payment, including any credit card or bank account number.

iv. *Transactional Information.* Microsoft and Google also typically retain certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through the website of Microsoft and Google).

v. *Customer Correspondence.* Microsoft and Google also typically maintain records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

vi. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

vii. *Google Drive Content.* Google provides users with a certain amount of free “cloud” storage, currently 15 gigabytes, through a service called “Google Drive” (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud” (that is, online). A user can access content stored on Google Drive by logging into his Google account through any computer or other electronic device connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

viii. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

ix. *Google Photos.* Google provides users with a certain amount of free storage that allows for users to store and share digital photographs. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

x. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

xi. *YouTube Content.* Google allows subscribers to maintain linked YouTube accounts, a global video-sharing website that allows users to upload and share videos with the public on the Internet. Registered users can upload an unlimited number of videos and add comments to videos.

xii. *Google Chats and Google Hangouts Content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

xiii. *Web History.* Google maintains searches and account browsing activity, from Chrome, Google’s proprietary web browser, as well as other Google applications.

xiv. *Location History.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device’s most recent location data in connection with a Google account.

xv. *Android Services.* Google also maintains information relating to Android, as it relates to an account. Android is a mobile operating system that is developed by Google, and is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI (International Mobile Station Equipment Identifier), MEID (Mobile Equipment Identifier), device ID, and/or serial number of the device. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

xvi. *Preserved and Backup Records.* The Providers also maintain preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). The Providers may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

#### **D. Services and Records of Dropbox**

6. I have learned the following about Dropbox:

a. Dropbox is a file synchronizing and collaboration service that allows users to store, access, and share files on computers, phones, tablets, and the Dropbox website. Dropbox creates a folder on the user's computer, the contents of which are then synchronized to Dropbox's servers and to other computers and devices on which the user has installed Dropbox, keeping the same files up-to-date on all devices.

b. Users may save and share a variety of file types in Dropbox accounts, including videos, images, audio files, and text files.



c. Dropbox users are able to share files by creating “shared folders” within the user’s Dropbox account. Users can then circulate electronic links to others via the Internet, enabling the recipients of those links to access and, in some cases, edit the shared files.

d. Dropbox maintains the following categories of records for its users:

i. *Subscriber Information.* Dropbox maintains records of subscriber information for its users, including: (1) names provided by the Dropbox user; (2) email addresses provided by the Dropbox user; (3) the time and date of account registration; (4) the type of account; (5) the IP address recorded for the last account access; (6) IP addresses recorded for account logins; and (7) devices associated with a Dropbox account.

ii. *User Activity Log.* Dropbox maintains logs of actions taken by users within a Dropbox account without reference to any filenames. This information may include records of login times and methods used to connect to the account (such as logging into the account through Dropbox’s website).

iii. *File Activity Log.* Dropbox maintains file account activity, such as dates and times when files were deleted or added, or when a shared folder was added to the user’s account.

iv. *Customer Correspondence.* Dropbox typically maintains records of any customer service contacts with or about the user, including any inquiries or complaints concerning the user’s account.

v. *Account Content.* Dropbox maintains content information for its users, including audio, video, image, and text files shared and saved through Dropbox.

vi. *Preserved and Backup Records.* Dropbox maintains preserved copies of the above-described categories of records with respect to a user account, for at least 90 days, upon

receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Dropbox may also maintain backup copies of the above-described categories of records pursuant to its own data retention policy.

#### **E. Services and Records of Twitter**

7. I have learned the following about Twitter:

a. Twitter offers electronic messaging and online social media services. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to post and read 140-character messages called “tweets,” and to restrict their “tweets” to individuals whom they approve. In addition, Twitter’s subscribers can send “direct messages,” or “DMs” to other subscribers, which are typically only viewable by the sender or recipient of the direct message. These features are described in more detail below. A subscriber using Twitter’s services can access his or her account from any computer connected to the Internet.

b. Twitter maintains the following records and information with respect to every subscriber account:

i. *Biographical Information.* Twitter allows its users to create personal profile pages. These pages include a short biography, photographs of the users, and location information for the user.

ii. *Tweets.* As discussed above, Twitter’s users can use their accounts to post “tweets” of 140 characters or fewer. Each tweet includes a timestamp that displays when the tweet was posted. Twitter’s users can also “favorite,” “retweet,” or reply to tweets of other users. In addition, when a tweet includes a username, often preceded by “@,” Twitter designates that

tweet a “mention” of the identified user. In the “Connect” tab for each account, Twitter provides the user with a list of other users who have favorite or retweeted the user’s own tweets, as well as a list of all tweets that include the user’s username (*i.e.*, a list of all mentions and replies for that username). By enabling the “Tweet With Location” feature, Twitter’s users can also choose to include location data in their tweets.

iii. *Photographs/Images.* Twitter users can also include photographs or images in their tweets. Each account is provided a user gallery, which stores photographs or images that the user has shared on Twitter’s network, including photographs or images that were uploaded from another service.

iv. *Link Information.* Twitter’s users can also include links to a website in their tweets. By using Twitter’s linking service, a longer website link can be converted into a shortened link, which allows it to fit into the 140-character limit. The linking service measures how many times a link has been clicked.

v. *Associated Users.* A user can also “follow” other users, which means that the user subscribes to the other users’ tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user’s “followers” list) and a list of people whom that user follows (*i.e.*, the user’s “following” list). Twitter’s users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that their tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A user can also group other users into “lists” that display on the right side of the user’s home page. Twitter also provides users with a list of “Who to Follow,” which includes recommendations of accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

vi. *Direct Messages.* A user can also send direct messages, or DMs, to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users.

vii. *Subscriber and Billing Information.* Twitter collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Twitter also maintains records concerning the date on which the account was created, the IP address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Twitter maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

viii. *Search Information.* Twitter includes a search function that enables its users to search all public tweets for keywords, usernames, or subject, among other things. A user may save up to 25 past searches.

ix. *Third-party Information.* Users can connect their accounts to third-party websites and applications, which may grant these websites and applications access to the users' public profiles with Twitter.

x. *Transactional Information.* Twitter also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Twitter's website).

xi. *Customer Correspondence.* Twitter also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

xii. *Preserved Records.* Twitter also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

#### **F. Services and Records of Instagram**

8. I have learned the following about Instagram:

a. Instagram operates a free social-networking application and website, accessed through applications for mobile devices and at Instagram.com, which is centered around photography. Instagram's users establish accounts and create profiles, which they can use to post and share photographs and other information from computers and other web-enabled devices, such as certain cellular phones. Instagram's application for mobile devices also includes a camera application, which can assist a user in taking pictures and posting the photographs to their Instagram account.

b. Instagram asks users to provide basic contact information to Instagram, either during the registration process or thereafter. This information may include the user's full name, contact e-mail addresses, telephone numbers, screen names, websites, and other personal identifiers.

c. Instagram users can adjust privacy settings for the photographs, communications and information associated with their accounts. By adjusting these privacy settings, a user can, for example, require authorization before anyone can follow, or have access

to, photographs posted by the user. Instagram accounts also include other account settings that users can adjust, to control, for example, the types of notifications they receive from Instagram.

d. Instagram users may also “follow” other users. When a user “follows” another user, the user automatically receives photographs posted by the “followed” user. Depending on a user’s privacy settings, a request to “follow” may have to be accepted by the “followed” user, before the requesting user can view the “followed” user’s photographs.

e. Instagram users may comment on photographs posted by other users.

f. Instagram users have the option to upload photographs with geolocation information. Those photographs can then be added to a user’s “Photo Map,” allowing users with access to the photographs to see on a map where the photographs were uploaded to Instagram. Even if the user elects not to add a photograph to a “Photo Map,” the geolocation data is stored with the Photograph so long as that functionality is enabled.

g. Instagram users have access to a “News Feed,” which shows activity among a user’s network of followed users. The News Feed, among other things, displays photographs that others in the user’s network have liked and comments among individuals in a user’s network.

h. Instagram users may share their own photographs via other social networking services, such as Twitter and Facebook. Users may also share another user’s public photographs via Twitter.

i. Instagram also retains IP logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Instagram, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action.

j. Social-networking providers like Instagram typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Instagram's users may communicate directly with Instagram about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Instagram typically retain records about such communications, including records of contacts between the user and Instagram's support services, as well as records of any actions taken by Instagram or user as a result of the communications.

#### **G. Jurisdiction and Authority to Issue Warrants**

9. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Providers, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

10. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

11. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Providers from notifying the subscriber(s) or any other person of the warrant, for such period

as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

## **II.Factual Background**

12. On May 31, 2017, the Honorable Katharine A. Parker, United States Magistrate Judge, issued an arrest warrant based on a sealed Complaint (the “Complaint” or “Compl.”) that charged Ali Kourani with eight counts: (1) providing material support to an FTO, *i.e.*, Hizballah, in violation of Title 18, United States Code, Section 2339B; (2) conspiracy to provide material support and resources to an FTO, *i.e.*, Hizballah, in violation of Title 18, United States Code, Section 2339B; (3) receiving military-type training from an FTO, *i.e.*, Hizballah, in violation of Title 18, United States Code, Section 2339D; (4) conspiracy to receive military-type training from an FTO, *i.e.*, Hizballah, in violation of Title 18, United States Code, Sections 371 and 2339D; (5) conspiracy to possess, carry, and use firearms and destructive devices during and in relation to crimes of violence, in violation of Title 18, United States Code, Section 924(o); (6) making and receiving a contribution of funds, goods, and services to and from a specially designated terrorist, *i.e.*, Hizballah, in violation of Title 50, United States Code, Section 1705; (7) conspiracy to make and receive a contribution of funds, goods, and services to and from a specially designated terrorist, *i.e.*, Hizballah, in violation of Title 50, United States Code, Section 1705; and (8) naturalization fraud to facilitate an act of international terrorism, in violation of Title 18, United States Code, Section 1425. The Complaint, which was filed on May 31, 2017 and docketed 17 Mag. 4151, is attached hereto as Exhibit A and incorporated by reference.

13. As alleged in the Complaint:

a. Kourani was a member of the Islamic Jihad Organization (“IJO”), which is a highly compartmentalized component of Hizballah (an FTO) that is responsible for the planning,



preparation, and execution of intelligence, counterintelligence, and terrorist activities outside of Lebanon. (*See* Compl. ¶¶ 16, 17, 19). Beginning in approximately 2000, Kourani obtained training from Hizballah and the IJO in tradecraft, weapons, and military tactics. Kourani later identified himself to the FBI as an IJO “sleeper” operative working undercover in the United States. (*See id.* ¶¶ 16, 19, 25). Principally responsible for conducting IJO intelligence-gathering and surveillance activities, Kourani received taskings in Lebanon and executed his missions covertly. (*See id.* ¶ 16, 26). For example, Kourani gathered intelligence and conducted surveillance of U.S. military and intelligence outposts in New York City, as well as airports in New York City and elsewhere, in support of anticipated IJO terrorist attacks. (*See id.*).

b. Kourani used email accounts, at least one social media account, and electronic storage media to engage in activities on behalf of, and provide support to, Hizballah and the IJO. (*See, e.g.*, Compl. ¶¶ 22(a), 22(e), 26(e)).

c. Kourani searched for, and viewed, Hizballah- and IJO-related propaganda on the Internet, including videos that could be stored and shared using email accounts and social media accounts. (*See* Compl. ¶¶ 21(a)-(b), 21(d)-(h)).

d. Certain Google searches performed by Kourani, which were obtained previously pursuant to a search warrant relating to one of Kourani’s email accounts that is not among the Subject Accounts, serve as evidence of Kourani’s participation in the crimes charged in the Complaint. (*See, e.g.*, Compl. ¶ 27). For example, Kourani searched for the address of a U.S. government facility that he later admitted to surveilling on behalf of the IJO. (*See id.* ¶¶ 26(a), 27(f)).

14. Kourani was arrested in the Bronx on the morning of June 1, 2017. A Samsung smartphone capable of accessing the Internet was seized incident to his arrest.

15. Following Kourani's arrest, Kourani's apartment was searched by the FBI pursuant to a search warrant issued on May 31, 2017 by Judge Parker. The search revealed, among other things, two laptop computers that Kourani appears to have used.

16. On June 2, 2017, in the presence of defense counsel, Kourani consented to searches of the Subject Accounts. The consent form signed by Kourani and his attorney is attached hereto as Exhibit B. Before signing the consent form, and in the presence of counsel, Kourani reviewed a list of the Subject Accounts, and confirmed that he had, at some time between 2000 and the present, utilized the Subject Accounts. By signing the consent form, Kourani also affirmed: (i) "I have a right to access or use these . . . accounts and all information found in them"; (ii) "I understand that any contraband or evidence on these . . . accounts may be used against me in a court of law"; and (iii) "I relinquish any constitutional right to privacy in these . . . accounts and any information stored on them."

17. Based on my training and experience, notwithstanding Kourani's voluntary consent to searches of the Subject Accounts, the Providers will not provide the contents of the Subject Accounts to the Government or the FBI in the absence of a Court order such as a search warrant.

### **III.Evidence, Fruits and Instrumentalities Relating to the Subject Offenses**

18. Based upon the foregoing and the allegations in the Complaint attached as Exhibit A, I respectfully submit there is probable cause to believe that information stored on the Providers' servers, as more fully described in Section II of Attachment A to the proposed warrants, associated with the Subject Accounts will contain evidence, fruits, and instrumentalities of the Subject Offenses.<sup>2</sup> For example, the Subject Accounts likely contain information relating to Kourani's

---

<sup>2</sup> The Government is not relying on Kourani's consent to search the Subject Accounts as a basis for establishing probable cause to support the issuance of the warrant.

physical location at times relevant to the Subject Offenses, such as IP address information, photographs, and communications, which corroborates, for example, his travel to Lebanon for meetings with Hizballah and IJO personnel. The Subject Accounts that are email accounts with usernames relating to business ventures associated with Kourani, such as jacobfashion@hotmail.com, holy.smoke.shop.franklin@gmail.com, and wmc.sportswear@gmail.com, are likely to contain information relating to financial transactions that will provide information relating to bank accounts and other means of effecting funds transfers used by Kourani, which may in turn lead to evidence relating to the Subject Offenses. The Subject Accounts that are email accounts maintained by Google may contain additional information relating to Google searches conducted by Kourani relating to the Subject Offenses.

19. Accordingly, I respectfully submit that there is probable cause to believe that, within the Subject Accounts, there are:

- communications relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government;
- evidence of the identity(ies) of the user(s) of the Subject Accounts;
- evidence of the identities and locations of co-conspirators in the Subject Offenses, including photographs of and communications with such individuals;
- evidence of participation in the Subject Offenses by the user(s) of the Subject Accounts and others, including records relating to travel and financial transactions in furtherance of the Subject Offenses;

- evidence related to banks and other financial institutions at which the user(s) of the Subject Accounts conduct business, including, potentially, transactions in furtherance of the Subject Offenses;
- evidence of other online accounts the user(s) of the Subject Accounts, including potentially for operational activity or otherwise in furtherance of the Subject Offenses; and
- passwords or other information needed to access user's computer or other online accounts.

#### **IV. Review of the Information Obtained Pursuant to the Warrants**

20. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrants requested herein will be transmitted to the Providers, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 30 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrants, a copy of which shall not be transmitted to the Providers.

21. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is

analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

#### **V. Request for Sealing**

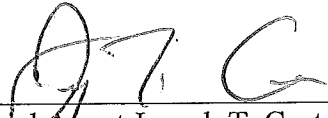
22. The scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

23. Accordingly, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those


materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

#### **VI. Conclusion**

24. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

  
Special Agent Joseph T. Costello, FBI

Sworn to before me this  
6th day of June, 2017

  
~~HONORABLE GABRIEL W. GORENSTEIN~~  
United States Magistrate Judge *HENRY PITMAN*  
Southern District of New York

# EXHIBIT A

17 MAG 4151

Approved: Amanda L. Houle  
 EMIL J. BOVE III / AMANDA L. HOULE  
 Assistant United States Attorneys

Before: HONORABLE KATHARINE H. PARKER  
 United States Magistrate Judge  
 Southern District of New York

----- X  
 UNITED STATES OF AMERICA : SEALED COMPLAINT  
 :  
 - v. - : Violations of  
 : 18 U.S.C. §§ 2339B,  
 ALI KOURANI, : 2339D, 924(o), 1425(a);  
 a/k/a "Ali Mohamad Kourani," : 50 U.S.C. § 1705(a)  
 a/k/a "Jacob Lewis," :  
 a/k/a "Daniel," : COUNTIES OF OFFENSE:  
 : NEW YORK, BRONX  
 Defendant. :  
 ----- X

STATE OF NEW YORK )  
 ) ss.:  
 COUNTY OF NEW YORK )

JOSEPH T. COSTELLO, being duly sworn, deposes and says that he is a Special Agent at the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE

(Provision of Material Support to Hizballah,  
 a Designated Foreign Terrorist Organization)

1. From at least in or about 2002, up to and including in or about September 2015, in the Southern District of New York, Lebanon, and elsewhere, and in an offense begun and committed outside of the jurisdiction of any particular State or district of the United States, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, who is expected to be first arrested in the Southern District of New York, knowingly did provide and attempt to provide, and aided and abetted the provision of, "material support or resources," as that term is defined in Title 18, United States Code, Section 2339A(b), to a foreign terrorist organization, to wit, Hizballah, which has been designated by the Secretary of State as a foreign terrorist



organization since 1997, pursuant to Section 219 of the Immigration and Nationality Act ("INA"), and is currently designated as such as of the date of the filing of this Complaint, including, among other things, personnel, knowing that Hizballah was a designated foreign terrorist organization (as defined in Title 18, United States Code, Section 2339B(g)(6)), that Hizballah engages and has engaged in terrorist activity (as defined in section 212(a)(3)(B) of the INA), and that Hizballah engages and has engaged in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989).

(Title 18, United States Code, Sections 2339B(a)(1), (d)(1)(A), (d)(1)(C), (d)(1)(D), (d)(1)(E), (d)(1)(F), (d)(2), 3238, and 2.)

### COUNT TWO

(Conspiracy to Provide Material Support to Hizballah,  
a Designated Foreign Terrorist Organization)

2. From at least in or about 2002, up to and including in or about September 2015, in the Southern District of New York, Lebanon, and elsewhere, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, who is expected to be first arrested in the Southern District of New York, and others known and unknown, knowingly did combine, conspire, confederate and agree together and with each other to provide "material support or resources," as that term is defined in Title 18, United States Code, Section 2339A(b), to a foreign terrorist organization, to wit, Hizballah, which has been designated by the Secretary of State as a foreign terrorist organization since 1997, pursuant to Section 219 of the INA, and is currently designated as such as of the date of the filing of this Complaint.

3. It was a part and an object of the conspiracy that ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, and others known and unknown, would and did agree to provide Hizballah with material support and resources, including personnel, knowing that Hizballah was a designated foreign terrorist organization (as defined in Title 18, United States Code, Section 2339B(g)(6)), that Hizballah engages and has engaged in terrorist activity (as defined in section 212(a)(3)(B) of the INA), and that Hizballah engages and has engaged in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989), in violation of Title 18, United States Code, Section 2339B.

4. In furtherance of the conspiracy and to effect the illegal object thereof, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, and others known and unknown, committed the overt acts set forth below, among others:

a. From at least in or about 2009, up to and including in or about September 2015, KOURANI conducted surveillance of U.S. military and intelligence outposts in New York City, as well as airports in New York City and another country, in support of anticipated terrorist attacks by Hizballah's Islamic Jihad Organization.

b. In or about July 2011, KOURANI attended a military training camp in the vicinity of Birkat Jabrur, Lebanon, which was operated by Hizballah's Islamic Jihad Organization, where KOURANI was provided with military-tactics and weapons training.

(Title 18, United States Code, Sections 2339B(a)(1), (d)(1)(A), (d)(1)(C), (d)(1)(D), (d)(1)(E), (d)(1)(F), (d)(2), and 3238.)

**COUNT THREE**

(Receipt of Military-type Training from Hizballah,  
a Designated Foreign Terrorist Organization)

5. In or about 2011, in Lebanon and elsewhere, and in an offense begun and committed outside of the jurisdiction of any particular State or district of the United States, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, who is expected to be first arrested in the Southern District of New York, knowingly received military-type training from and on behalf of Hizballah, which has been designated by the Secretary of State as a foreign terrorist organization since 1997, pursuant to Section 219 of the INA, and is currently designated as such as of the date of the filing of this Complaint, knowing that Hizballah was a designated foreign terrorist organization (as defined in Title 18, United States Code, Section 2339D(c)(4)), that Hizballah engages and has engaged in terrorist activity (as defined in section 212 of the INA), and that Hizballah engages and has engaged in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989), to wit, KOURANI received training in the use of weapons and military tactics from other members of Hizballah.

(Title 18, United States Code, Sections 2339D(a), (b)(1), (b)(3), (b)(4), (b)(5), (b)(6), 3238, and 2.)

COUNT FOUR

(Conspiracy to Receive Military-type Training from Hizballah,  
a Designated Foreign Terrorist Organization)

6. In or about 2011, in Lebanon and elsewhere, and in an offense begun and committed outside of the jurisdiction of any particular State or district of the United States, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, who is expected to be first arrested in the Southern District of New York, and others known and unknown, knowingly did combine, conspire, confederate and agree together and with each other to receive military-type training from and on behalf of Hizballah, which has been designated by the Secretary of State as a foreign terrorist organization since 1997, pursuant to Section 219 of the INA, and is currently designated as such as of the date of the filing of this Complaint.

7. It was a part and an object of the conspiracy that ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, and others known and unknown, would and did receive military-type training from and on behalf of Hizballah, knowing that Hizballah was a designated foreign terrorist organization (as defined in Title 18, United States Code, Section 2339D(c)(4)), that Hizballah engages and has engaged in terrorist activity (as defined in section 212 of the INA), and that Hizballah engages and has engaged in terrorism (as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989), in violation of Title 18, United States Code, Section 2339D.

8. In furtherance of the conspiracy and to effect the illegal object thereof, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, and others known and unknown, committed the overt acts set forth in paragraph 4, supra, which are fully incorporated by reference herein, among others.

(Title 18, United States Code, Sections 371, 2339D(a), (b)(1),  
(b)(3), (b)(4), (b)(5), (b)(6), and 3238.)

COUNT FIVE

(Conspiracy to Possess, Carry, and Use Machine Guns and Destructive Devices During and in Relation to Crimes of Violence)

9. From at least in or about 2002, up to and including in or about September 2015, in the Southern District of New York, Lebanon, and elsewhere, and in an offense begun and committed outside of the jurisdiction of any particular State or district of the United States, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, who is expected to be first arrested in the Southern District of New York, and others known and unknown, knowingly did combine, conspire, confederate, and agree together and with each other to violate Title 18, United States Code, Section 924(c).

10. It was a part and an object of the conspiracy that ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, and others known and unknown, during and in relation to a crime of violence for which KOURANI may be prosecuted in a court of the United States, namely, the offenses charged in Counts One, Two, Three, and Four of this Complaint, would and did use and carry machine guns and destructive devices, to wit, firearms that were capable of automatically firing more than one shot without manual reloading, including an AK-47 assault rifle, an MP5 submachine gun, and a Russian PKS machine gun, and destructive devices, including rocket-propelled grenade launchers ("RPGs"), and, in furtherance of such crime of violence, possess machine guns and destructive devices, in violation of Title 18, United States Code, Sections and 924(c)(1)(A) and 924(c)(1)(B)(ii).

(Title 18, United States Code, Sections 924(o) and 3238.)

COUNT SIX

(Making or Receiving a Contribution of Funds, Goods, and Services to and from Hizballah, in Violation of the International Emergency Economic Powers Act)

11. From at least in or about 2002, up to and including in or about September 2015, in the Southern District of New York, Lebanon, and elsewhere, and in an offense begun and committed outside of the jurisdiction of any particular State or district of the United States, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, a United States

person, who is expected to be first arrested in the Southern District of New York, willfully attempted to and did make and receive a contribution of funds, goods, and services to and for the benefit of, as well as from, Hizballah, a specially designated terrorist, in that KOURANI attempted to and did provide to Hizballah personnel and services.

(Title 50, United States Code, Section 1705(a); Title 18, United States Code, Sections 3238 and 2; and Title 31, Code of Federal Regulations, Sections 595.204, 595.205, and 595.311.)

**COUNT SEVEN**

(Conspiracy to Make or Receive a Contribution of Funds, Goods, and Services to and from Hizballah, in Violation of the International Emergency Economic Powers Act)

12. From at least in or about 2002, up to and including in or about September 2015, in the Southern District of New York, Lebanon, and elsewhere, and in an offense begun and committed outside of the jurisdiction of any particular State or district of the United States, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, a United States person, who is expected to be first arrested in the Southern District of New York, knowingly and willfully, along with others known and unknown, did combine, conspire, confederate, and agree together and with each other to make and receive a contribution of funds, goods, and services to and for the benefit of, as well as from, Hizballah, a specially designated terrorist, by agreeing with others to provide to Hizballah personnel and services, and to receive funds from Hizballah.

(Title 50, United States Code, Section 1705(a); Title 18, United States Code, Section 3238; and Title 31, Code of Federal Regulations, Sections 595.204, 595.205, and 595.311.)

**COUNT EIGHT**

(Unlawful Procurement of Citizenship or Naturalization to Facilitate an Act of International Terrorism)

13. In or about 2009, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, in the Southern District of New York and elsewhere, knowingly procured and attempted to procure, contrary to law, the naturalization of any person to facilitate an act of international terrorism as defined in Title 18, United States Code, Section 2331, to wit,

KOURANI submitted a naturalization application for himself containing false statements relating to, among other things, his membership in and provision of material support and resources to Hizballah.

(Title 18, United States Code, Sections 1425(a), 3291, and 2.)

The bases for my knowledge and the foregoing charges, are, in part, as follows:

14. I have been a Special Agent at the FBI since approximately 2014. Prior to joining the FBI, I served as a Special Agent with the U.S. Department of State, Diplomatic Security Service, for approximately five years. For the last approximately two years, I have been assigned to the FBI's New York Joint Terrorism Task Force ("JTTF"). The focus of my counterterrorism and counterintelligence efforts has been investigating and disrupting terrorist activities by Hizballah and, in particular, Hizballah's Islamic Jihad Organization ("IJO").

15. I have learned the facts contained in this Complaint from, among other sources, my personal participation in this and related investigations, my discussions with other law enforcement personnel, searches in which I have participated, surveillance in which I have participated, and my review of documents and other materials. Because this Complaint is being submitted for the limited purpose of establishing probable cause, it does not include every fact that I have learned during the course of this investigation. Further, any statements related herein are described in substance and in part only.

#### INTRODUCTION

16. The FBI's investigation revealed that ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, was a member of the IJO, which is a highly compartmentalized component of Hizballah responsible for the planning, preparation, and execution of intelligence, counterintelligence, and terrorist activities outside of Lebanon. Beginning in approximately 2000, KOURANI obtained training from Hizballah and the IJO in tradecraft, weapons, and military tactics. KOURANI later identified himself to the FBI as an IJO "sleeper" operative working undercover in the United States. Principally responsible for conducting IJO intelligence-gathering and surveillance activities, KOURANI received taskings in Lebanon and executed his missions covertly. For example, KOURANI gathered



intelligence and conducted surveillance of U.S. military and intelligence outposts in New York City, as well as airports in New York City and elsewhere, in support of anticipated IJO terrorist attacks.

**HIZBALLAH, AL MANAR, AND THE ISLAMIC JIHAD ORGANIZATION**

17. Based on my training and experience, my participation in this and related investigations, and my review of publicly available documents, reports, and other materials, I understand the following, in substance and in part:

a. Hizballah is a Lebanon-based Shia Islamic organization with political, social, and terrorist components. Hizballah was founded in the early 1980s with support from Iran after the 1982 Israeli invasion of Lebanon, and its mission includes establishing a fundamentalist Islamic state in Lebanon. In 1997, the U.S. Department of State designated Hizballah a Foreign Terrorist Organization, pursuant to Section 219 of the INA, and it remains so designated today. In 2001, pursuant to Executive Order 13,224, the U.S. Department of the Treasury designated Hizballah a Specially Designated Global Terrorist entity. In 2010, State Department officials described Hizballah as the most technically capable terrorist group in the world, and a continued security threat to the United States.

b. Al Manar is a media organization controlled by the Iran-funded Hizballah terrorist network. Al Manar employs Hizballah personnel, supports fundraising and recruitment for Hizballah, and at least one Al Manar employee engaged in operational surveillance activities on behalf of Hizballah under cover of employment by Al Manar. In 2006, pursuant to Executive Order 13,224, the U.S. Department of the Treasury designated Al Manar a Specially Designated Global Terrorist entity.

c. The IJO, which is also known as the External Security Organization and "910," is a component of Hizballah responsible for the planning and coordination of intelligence, counterintelligence, and terrorist activities on behalf of Hizballah outside of Lebanon. IJO operatives are typically assigned a Lebanon-based "handler," sometimes referred to as a mentor, responsible for providing taskings, debriefing operatives, and arranging training. IJO often conducts targeted operations in stages, sending waves of one or more operatives with separate taskings such as surveillance, obtaining and storing necessary components and equipment, and attack execution.

d. Since Hizballah's formation, the organization has been responsible for numerous terrorist attacks that have killed hundreds, including the 1983 bombing of the United States Marine barracks in Lebanon, which killed 241 Marines; the 1983 bombing of the United States Embassy in Beirut, which killed 24 people; the 1985 hijacking of TWA Flight 847, which killed one U.S. citizen; the 1992 bombing of the Israeli Embassy in Argentina, which killed 29 people; and the 1994 bombing of a Jewish cultural center in Buenos Aires, which killed 95 people.

e. In July and August 2006, Hizballah and Israel engaged in armed conflict (the "2006 Lebanon War"), resulting in numerous casualties, after an incident on or about July 12, 2006 when Hizballah attacked Israeli Defense Force ("IDF") personnel. A ceasefire brokered by the United Nations went into effect on August 14, 2006.

f. In January 2012, Hussein Atris, an IJO operative with dual Lebanese-Swedish citizenship, was detained in Thailand as he tried to board a flight at a Bangkok airport. Atris subsequently led law enforcement personnel to a commercial building near Bangkok that housed a cache of nearly 10,000 pounds of urea-based fertilizer and 10 gallons of ammonium nitrate, which are chemicals that I know, based on my training and experience, can be used to construct explosives. The ammonium nitrate was stored in First Aid ice packs manufactured by a Guangzhou, China-based company ("Guangzhou Company-1").

g. In July 2012, Mouhamad Hassan Mouhamad El Hussein, an IJO operative with dual Lebanese-French citizenship, detonated explosives on a bus transporting Israeli tourists in the vicinity of an airport in Burgas, Bulgaria. Six people were killed and 32 others were injured. Law enforcement authorities recovered three fraudulent, purportedly U.S.-based, driver's licenses during the investigation, subsequently linked the attack to the IJO, and determined that ammonium nitrate was an active ingredient in the explosives.

h. Also in July 2012, Hossam Taleb Yaacoub, an IJO operative with dual Lebanese-Swedish citizenship, was arrested after conducting surveillance of Israeli tourists in the vicinity of an airport in Larnaca, Cyprus. Law enforcement authorities seized from Yaacoub a notebook containing coded entries relating to, among other things, Israeli tour busses. In March 2013, Yaacoub was convicted of crimes in Cyprus relating to these activities on behalf of the IJO.



i. In May 2015, Hussein Bassam Abdallah, an IJO operative with dual Lebanese-Canadian citizenship, was arrested in Cyprus after Cypriot authorities seized from an apartment rented by Abdallah approximately 8.2 tons of ammonium nitrate, at least some of which was stored in First Aid ice packs manufactured by Guangzhou Company-1, the manufacturer of the First Aid ice packs seized in Thailand in January 2012. See paragraph 17(f), supra. Abdallah possessed a copy of a fraudulent passport at the time of his arrest, and he was subsequently convicted of crimes in Cyprus relating to these activities on behalf of the IJO.

**THE DEFENDANT**

18. Based on my review of documents and information maintained by federal and state authorities in the United States, I am aware of the following:

a. ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, was born in the vicinity of Bint Jbeil, Lebanon in 1984.

b. In 2003, KOURANI lawfully entered the United States using a Lebanese passport. In the United States, KOURANI obtained a Bachelor of Science in biomedical engineering in 2009, and a Masters of Business Administration in 2013.

c. In April 2009, KOURANI became a naturalized citizen of the United States, see paragraph 20(c), infra.

d. KOURANI's U.S. and Lebanese passports reflect, among other things, travel to Lebanon at least approximately once annually between 2005 and 2015, and to Guangzhou, China in May 2009.

**THE DEFENDANT'S RECRUITMENT AND TRAINING BY**  
**HIZBALLAH AND THE IJO**

19. Based on my participation in interviews of ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, as well as my review of reports relating to interviews of KOURANI,<sup>1</sup> I know that KOURANI provided the following information to law enforcement, in substance and in part:

a. KOURANI considers his family name to be akin to the "Bin Ladens of Lebanon," and one of his brothers is the "face of Hizballah" in Yatar, Lebanon.

b. In approximately 2000, three years before entering the United States, see paragraph 18(b), supra, KOURANI attended a 45-day Hizballah "boot camp" in Lebanon. KOURANI was approximately 16 years old at the time, and he was permitted to attend because of his family's connections to a high-ranking Hizballah official named Haider Kourani. During the training, KOURANI was taught to fire AK-47 assault rifles and rocket launchers, as well as basic military tactics, by Hizballah personnel wearing uniforms.

c. KOURANI was in Southern Lebanon during the 2006 Lebanon War, see paragraph 17(e), supra, and his family's home was destroyed by an Israeli bombing during the conflict. KOURANI fled the area with relatives, and he returned to the United States via Syria.

d. In approximately 2008, KOURANI was recruited by Sheikh Hussein Kourani in Lebanon to join the IJO. KOURANI considered the IJO to be responsible for "black ops" on behalf of Hizballah and "the Iranians." By the time KOURANI joined the IJO, he understood that Hassan Nasrallah, the Secretary-General of

---

<sup>1</sup> ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, made statements to the FBI during multiple voluntary interviews in 2016 and 2017. The interviews in 2016 were conducted in a non-custodial setting. Five interviews were conducted in 2017 after an attorney representing KOURANI contacted the FBI and explained, in substance and in part, that KOURANI wished to provide information to the FBI in the hope of obtaining financial support and immigration benefits for certain of his relatives. No promises were made to KOURANI regarding such benefits, and the five interviews in 2017 were conducted in the attorney's presence, at the attorney's office, in a non-custodial setting.

Hizballah, operated the IJO and reported directly to Ali Khamenei, the Supreme Leader of Iran.

e. KOURANI believes that he was recruited to join the IJO in light of his education and residence in the United States, and in connection with efforts by the IJO to develop "sleepers" who maintained ostensibly normal lives but could be activated and tasked with conducting IJO operations.

f. Following KOURANI's initial recruitment by the IJO, KOURANI participated in a series of interviews in Lebanon with IJO personnel during which he was asked about his background, religious practices, and travel history, as well as provided with training on topics such as conducting interrogations, resisting interrogations, and surveillance techniques.

g. KOURANI was subsequently driven, while wearing a blacked-out motorcycle helmet, to a meeting with the man who acted as his IJO handler, whom KOURANI knew as "Fadi" and "Hajj" ("Fadi"). Fadi typically wore a mask during their meetings, and explained to KOURANI early in their relationship that the "golden rule" of the IJO was that "the less you know the better it is." Fadi acted as KOURANI's IJO handler until approximately September 2015, when KOURANI claims that he (KOURANI) was deactivated by the IJO.

h. One of Fadi's first instructions to KOURANI, who was a lawful permanent resident at the time, was to obtain United States citizenship and a U.S. passport as soon as possible.

i. Fadi later instructed KOURANI to obtain a U.S. passport card that could be used to re-enter the United States if his U.S. passport was seized outside the United States. Specifically, Fadi told KOURANI that he could use his Lebanese passport to fly to Mexico or Canada, and then enter the United States at a land border using the U.S. passport card.

j. KOURANI used at least two email addresses ("Kourani Email-1" and "Kourani Email-2") to communicate with IJO personnel abroad regarding his status and activities.

20. Based on my review of documents and information maintained by federal and state authorities in the United States, I am aware of the following:

a. ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, departed Lebanon, via Beirut-Rafic Hariri International Airport, in approximately late-January 2008.

b. In approximately August 2008, KOURANI submitted an application for naturalization in the United States (the "Naturalization Application"). KOURANI certified on the Naturalization Application, under penalty of perjury, that the information provided was true and correct. In the Naturalization Application, KOURANI made the following declarations, among others:

i. He had never "been a member of or in any way associated (either directly or indirectly) with . . . [a] terrorist organization."

ii. He had never "given false or misleading information to any U.S. government official while applying for any immigration benefit . . . ."

iii. He had never "lied to any U.S. government official to gain entry or admission into the United States."

c. On or about April 15, 2009, the Naturalization Application was approved, and KOURANI became a naturalized citizen of the United States.<sup>2</sup>

d. On or about April 15, 2009, KOURANI submitted an application for a U.S. passport, attaching the naturalization certificate that he was issued on the same day. In the passport application, KOURANI claimed, under penalty of perjury, that he had "no plans yet" with respect to foreign travel.

e. On or about April 22, 2009, KOURANI was issued a U.S. passport.

f. On April 30, 2009, KOURANI was issued a visa to enter China that was valid until October 30, 2009.

---

<sup>2</sup> The Naturalization Application was processed, in part, at a Manhattan office of the U.S. Citizenship and Immigration Services. ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, admitted to the FBI in 2017 that he understood that the Naturalization Application would be processed, at least in part, in the Southern District of New York.

g. On or about May 3, 2009, KOURANI entered China at an airport in Guangzhou, the location of Guangzhou Company-1, i.e., the manufacturer of the ammonium nitrate-based First Aid ice packs seized in connection with thwarted IJO attacks in Thailand and Cyprus, see paragraphs 17(f) and 17(i), supra.

h. In approximately April 2013, KOURANI obtained a U.S. passport card by relying on his naturalization certificate as an identification document.

21. Based on my review of documents and information relating to Kourani Email-1, which were produced by an Internet services provider, I am aware of the following:

a. In approximately late-January 2008, just days after ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, left Lebanon following his recruitment by the IJO, see paragraphs 19(d) and 20(a) supra, KOURANI conducted a series of Internet searches relating to the 2006 Lebanon War, including the terms "vinograd report" and "lebanon second war." Based on publicly available reporting, I know that Judge Eliyahu Winograd led the Commission to Investigate the Lebanon Campaign in 2006, i.e., the 2006 Lebanon War, which issued interim and final reports relating to the conflict.

b. Beginning in approximately May 2008, KOURANI conducted Internet searches and visited websites relating to Al Manar, the Specially Designated Global Terrorist entity that acts as a propaganda arm of Hizballah, see paragraph 17(b), supra. KOURANI conducted similar searches relating to Al Manar in approximately October 2012 and approximately March 2015.

c. Beginning on or about April 29, 2009, just one day before KOURANI obtained a visa to enter China, see paragraph 20(f), supra, he conducted Internet searches relating to the city of Guangzhou, China.

d. In approximately January 2013, KOURANI conducted an Internet search, in Arabic, and visited a website relating to Rabee Fares. The website KOURANI visited contains multiple images of Fares posing with weapons and military gear, and indicates that Fares was a member of Hizballah who was killed while fighting in

Syria approximately two days before KOURANI's Internet search.<sup>3</sup>

e. In approximately January 2013, KOURANI conducted an Internet search, in Arabic, for the phrase "if Hizballah was defeated," and visited a website with a Hizballah propaganda video produced by Al Manar featuring, among other things, a statement from Hizballah Secretary-General Nasrallah.

f. In approximately March 2013, KOURANI conducted an Internet search, in Arabic, relating to IJO operative Hossam Taleb Yaacoub, who was arrested in Cyprus in July 2012 based on his surveillance of Israeli targets in Cyprus, see paragraph 17(h), supra.

g. In approximately January 2014, KOURANI conducted an Internet search, in Arabic, and visited a website relating to prayers for victory over "the enemy."

h. In approximately March 2015, KOURANI conducted an Internet search, in Arabic, for the phrase "martyr leader Khattar Abdullah." Based on publicly available reporting, Khattar Abdullah was a Hizballah commander born near the same city in Lebanon as KOURANI, Bint Jbeil, and Abdullah was killed during battle in Syria in approximately March 2015.

**THE DEFENDANT'S USE OF IJO**  
**COMMUNICATIONS SECURITY AND TRADECRAFT**

22. Based on my participation in interviews of ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, as well as my review of reports relating to interviews of KOURANI, I know that KOURANI provided the following information to law enforcement, in substance and in part:

a. KOURANI was instructed by IJO personnel abroad to use digital storage media, such as USB drives and memory cards, to transport pictures and data back to Lebanon relating to his external operations.

b. In order to establish contact with Fadi when KOURANI returned to Lebanon, KOURANI would call a telephone number associated with a pager (the "IJO Pager") and provide a code that he understood was specific to him. After KOURANI called the IJO

---

<sup>3</sup> All translations set forth herein are preliminary and in draft form.

Pager, Fadi would contact KOURANI to set up an in-person meeting by calling a phone belonging to one of KOURANI's relatives.

c. KOURANI and Fadi used code during operational communications when KOURANI was outside of Lebanon. Initially, the code involved Fadi using marriage-related code, such as "bride," to signal to KOURANI that he should return to Lebanon. After KOURANI married, Fadi communicated similar recall messages using coded references to a "job" or "employment" prospect in Lebanon.

d. KOURANI also provided Fadi with the name of a particular childhood friend of KOURANI, and Fadi established one or more email accounts using that name for purposes of operational communications while KOURANI was outside of Lebanon. KOURANI deleted electronic communications from Fadi immediately after reviewing them.

e. In approximately 2011 or 2012, Fadi instructed KOURANI not to use existing operational email accounts or the IJO Pager, as the IJO assessed that these communications selectors had been compromised. KOURANI and Fadi did not use email to communicate regarding IJO operations after approximately 2012.

23. Based on my review of documents and information relating to Kourani Email-1 and Kourani Email-2 as well as other email accounts, which were produced by Internet service providers, I am aware of the following:

a. The email contacts stored in Kourani Email-2 contained two email addresses ("Fadi Email-1" and "Fadi Email-2") with usernames that are similar to the name of the childhood friend that ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, identified to Fadi, see paragraph 22(d), supra.



b. The contact for Fadi Email-1 was first saved in the account associated with Kourani Email-2 in approximately March 2008, and the contact entry relating to Fadi Email-1 was last modified on or about July 1, 2012.

c. Fadi Email-2 was created on or about October 15, 2011, and the user of the account indicated that he or she was based in Lebanon. The contact for Fadi Email-2 was first saved in the account associated with Kourani Email-2 on or about October 19, 2011. Like Fadi Email-1, the contact entry relating to Fadi Email-2 was last modified on or about July 1, 2012.

d. Consistent with Fadi's instruction that IJO operational email accounts had been compromised in approximately 2011 or 2012, see paragraph 22(e), supra, there was no message content stored in Kourani Email-2, Fadi Email-1, or Fadi Email-2, as of approximately May 2017.

24. Based on my review of documents and information maintained by federal and state authorities in the United States, I know that, on or about September 18, 2015, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, departed Beirut, Lebanon, and entered the United States at John F. Kennedy International Airport ("JFK"). During a secondary inspection, law enforcement personnel determined that KOURANI's cellphone did not contain a memory card, but found a memory card secreted under a travel sticker affixed to KOURANI's U.S. passport. The personnel conducting the inspection did not search the contents of the SIM card.

#### **THE DEFENDANT'S ADDITIONAL IJO MILITARY TRAINING**

25. Based on my participation in interviews of ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, as well as my review of reports relating to interviews of KOURANI, I know that KOURANI provided the following information to law enforcement, in substance and in part:

a. In approximately July 2011, KOURANI attended an IJO military training camp, located in the vicinity of Birkat Jabrur, Lebanon, where he was provided with military-tactics and weapons training.

b. In order to get to the training camp, KOURANI was picked up by an unknown driver, in a van with blacked-out windows, in the vicinity of Nabatieh, Lebanon. KOURANI was provided with a black, balaclava-style mask, which he put on and then got in the



back of the van with approximately five or six other IJO operatives.

c. A total of between approximately 20 and 25 IJO operatives attended the military training at Birkat Jabrur, which lasted for approximately two days and two nights.

d. During the training, KOURANI used---and fired---several weapons. When interviewed by the FBI in 2017, KOURANI identified, through counsel, photographs of several of the weapons that he discharged during the 2011 IJO training, including an RPG, an AK-47 assault rifle, an MP5 submachine gun, a PKS machine gun (a Russian-made belt-fed weapon), and a Glock pistol. KOURANI knew that several of the weapons he used during the training (including the MP5, PKS, and AK-47) could be fired in "automatic" mode; he was taught that these firearms could be discharged more accurately in semi-automatic mode, and his IJO trainers were unhappy when KOURANI fired in automatic mode during the training.<sup>4</sup>

**THE DEFENDANT'S INTELLIGENCE-GATHERING ACTIVITIES IN THE  
UNITED STATES ON BEHALF OF THE IJO**

26. Based on my participation in interviews of ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, as well as my review of reports relating to interviews of KOURANI, I know that KOURANI provided the following information to law enforcement, in substance and in part:

a. Fadi directed KOURANI to surveil and collect information regarding military and intelligence targets in the New York City area. In response to this tasking, KOURANI conducted physical surveillance of the following targets: (i) a U.S. government facility, which includes FBI offices, in Manhattan, New York; (ii) an U.S. Army National Guard facility in Manhattan, New York; (iii) a U.S. Secret Service facility in Brooklyn, New York; and (iv) a U.S. Army Armory facility in Manhattan, New York ("U.S. Armory-1"). KOURANI used his phone to videotape activity around at least one of these surveillance targets, transferred the video footage to a memory card, and brought the memory card to Fadi and other IJO personnel in Lebanon. KOURANI also used the Internet to obtain images of at least one of these surveillance targets, and

---

<sup>4</sup> Based on my conversations with another agent who has expertise in firearms, as well as my training and experience, I understand that the AK-47 assault rifle, MP5 submachine gun, and PKS machine gun are each firearms capable of firing more than one round through a single function of the trigger without manual reloading.

he provided the images to Fadi and other IJO personnel in Lebanon.

b. When interviewed by the FBI in 2017, KOURANI identified, through counsel, photographs of the above-referenced four locations in New York City where he conducted surveillance for the IJO.

c. Fadi directed KOURANI to surveil and collect information regarding airports, including the layout of terminals, the locations of cameras and personnel, and other security features.<sup>5</sup> In response, KOURANI provided detailed information to Fadi regarding specific security protocols; baggage-screening and collection practices; and the locations of surveillance cameras, security personnel, law enforcement officers, and magnetometers at JFK and an international airport in another country.

d. Fadi directed KOURANI to cultivate contacts in the New York City area who could provide firearms for use in potential future IJO operations in the United States. KOURANI brought Fadi a list of individuals he believed could supply firearms, but Fadi rejected the candidates as unreliable.

e. Fadi directed KOURANI to identify and collect intelligence regarding individuals in the United States affiliated with the IDF. KOURANI believed that the IJO gave him this tasking to facilitate, among other things, assassinations of IDF personnel in retaliation for the 2008 assassination of Imad Mughniyah, the former leader of the IJO. KOURANI used a social media account to identify IDF members or associates in the New York City area, and he described his search methodology to Fadi.

f. Consistent with the fraudulent identification documents seized during the investigation of IJO activities in Bulgaria and Cyprus, see paragraphs 17(g) and 17(i), supra, Fadi asked KOURANI if KOURANI could obtain employment at a Department of Motor Vehicles office in order to facilitate efforts by the IJO to obtain fraudulent identification documents for use in operations. KOURANI told Fadi he could not do so because he believed that it would draw too much attention if someone with his educational background applied for such a clerical position.

g. Fadi directed KOURANI to obtain surveillance equipment in the United States, including drones, night-vision

---

<sup>5</sup> Based on my training and experience, I understand that a standard tasking to many IJO operatives is to surveil and collect information regarding airports.

goggles, and high-powered cameras, so that the underlying technology could be studied and replicated by the IJO.

27. Based on my review of documents and information relating to Kourani 'Email-1, which were produced by an Internet service provider, I am aware of the following:

a. In approximately April 2011, ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, viewed a series of Google Maps related to LaGuardia Airport in Queens, New York, some of which were zoomed in on the locations of terminals.

b. In approximately April 2012, KOURANI conducted a series of Internet searches, and viewed images, relating to sniper rifles.

c. In approximately May 2012, KOURANI visited the website of a company that sells weapons (including firearms), body armor, uniforms, and tactical gear.

d. In approximately February 2013, KOURANI used Google Maps to view an image of, among other things, a U.S. Armed Forces Career Center in Queens, New York.


e. In approximately February 2014, KOURANI visited a website with information relating to manufacturing, repairing, and operating drones.

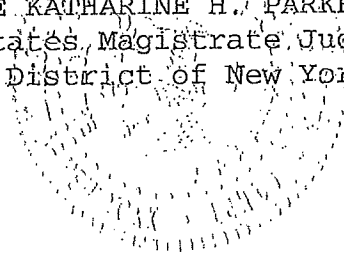
f. In approximately April 2014, KOURANI conducted an Internet search and visited a website relating to U.S. Armory-1, i.e., one of the locations that KOURANI told the FBI in 2017 that he surveilled, see paragraph 26(a), supra.

WHEREFORE, the deponent respectfully requests that a warrant be issued and that ALI KOURANI, a/k/a "Ali Mohamad Kourani," a/k/a "Jacob Lewis," a/k/a "Daniel," the defendant, be arrested and imprisoned, or bailed, as the case may be.

  
\_\_\_\_\_  
JOSEPH T. COSTELLO  
Special Agent, FBI

Sworn to before me this  
31st Day of May, 2017

  
\_\_\_\_\_  
HONORABLE KATHARINE H. PARKER  
United States Magistrate Judge  
Southern District of New York



# EXHIBIT B

## United States Department of Justice

### CONSENT TO SEARCH COMPUTER/ ELECTRONIC EQUIPMENT/SOCIAL MEDIA ACCOUNTS

I, Ali Kourani, have been asked to give my consent to a search. I have also been informed of my right to refuse to consent to such a search and discussed my rights with my attorney, Peggy Cross-Goldenberg.

I hereby authorize personnel from the Federal Bureau of Investigation ("FBI") and the United States Attorney's Office for the Southern District of New York ("USAO-SDNY") to search:

The following storage media or electronic devices:

SAMSUNG SM-G930T Cellphone with IMEI 355916071882540

Password: 8413

The following social media and electronic accounts:

ali.m.kourani@gmail.com

aliku@hotmai.com

jacobfashion@hotmail.com

holy.smoke.shop.franklin@gmail.com

jacob.kouran@gmail.com

wmc.sportswear@gmail.com

Dropbox account associated with ali.m.kourani@gmail.com

Dropbox account associated with aliku@hotmai.com

Twitter account associated with ali.m.kourani@gmail.com

Twitter account associated with aliku@hotmai.com

Instagram account associated with ali.m.kourani@gmail.com

Instagram account associated with aliku@hotmai.com

Instagram account associated with jacob.kouran@gmail.com

I consent that search may be for any purpose, and that the search may include the examination of computer data and the use of forensic review techniques. I consent to the search occurring at any time, for any length of time, and at any location.

If any of the devices/accounts described above are protected with a password and/or encrypted, I consent to the use of my passwords and/or encryption keys to access the data.

I certify that I have a right to access or use these devices/accounts and all information found in them. I understand that any contraband or evidence on these devices/accounts may be used against me in a court of law.

I relinquish any constitutional right to privacy in these devices/accounts and any information stored on them.

I authorize the FBI and the USAO-SDNY to search, and to make and keep a copy of any information stored on these devices/accounts.

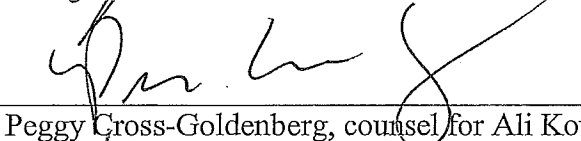
I understand that any such copy will not be my property and that I will have no privacy or possessory interest in the copy.

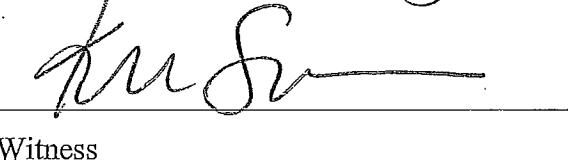
This written permission is given by me voluntarily. I have not been threatened, placed under duress, or promised anything in exchange for my consent. I have read this form, or it has been read to me, and I understand it.

I understand the English language and have been able to communicate with the agents/officers.

  
\_\_\_\_\_  
Ali Kourani

06/2/17  
\_\_\_\_\_  
Date and time

  
\_\_\_\_\_  
Peggy Cross-Goldenberg, counsel for Ali Kourani

  
\_\_\_\_\_  
Witness



17 MAG 4291

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of Warrants for All  
Content and Other Information  
Associated With Two Dropbox  
Accounts, Maintained at Premises  
Controlled by Dropbox, Inc.

### SEARCH WARRANT

TO: Dropbox, Inc. ("Provider")


Federal Bureau of Investigation ("Investigative Agency")

1. **Warrant.** Upon an Affidavit of a federal law enforcement officer in connection with an investigation being conducted by the Investigative Agency, pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe that the Dropbox accounts associated with the email addresses ali.m.kourani@gmail.com and alikuku@hotmail.com (the "Subject Accounts"), which are maintained at premises controlled by the Provider, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

6-6-17      5:02 PM  
Date Issued      Time Issued

  
\_\_\_\_\_  
HONORABLE HENRY B. PITMAN  
United States Magistrate Judge  
Southern District of New York

## **Search Warrant Attachment A**

### **I. Subject Accounts and Execution of Warrant**

This warrant is directed to Dropbox, Inc. (the “Provider”), with offices in San Francisco, California, and applies to all content and other information within the Provider’s possession, custody, or control associated with the Dropbox accounts associated with the email addresses ali.m.kourani@gmail.com and alikuku@hotmail.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, which is not to be transmitted to the Provider.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Subscriber Information.* All subscriber information associated with the Subject Accounts, including: (1) names provided by the Dropbox user; (2) email addresses provided by the Dropbox user; (3) the time and date of account registration; (4) the type of account; (5) the IP address recorded for the last account access; (6) IP addresses recorded for account logins; and (7) devices associated with a Dropbox account.

b. *User Activity Log.* Logs of actions taken by users of the Subject Accounts, including records of login times and methods used to connect to the account (such as logging into the account through Dropbox’s website).

c. *File Activity Log*. All records relating to file account activity associated with the Subject Accounts, including dates and times when files were deleted or added, or when a shared folder was added to the user's account.

d. *Customer Correspondence*. Records of any customer service contacts with or about the user of the Subject Accounts.

e. *Account Content*. All content information associated with the Subject Accounts, including audio, video, image, and text files shared and saved through Dropbox.

f. *Preserved and Backup Records*. Any preserved copies of the foregoing categories of records with respect to the Subject Accounts.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of (i) Title 18, United States Code, Section 2339B (providing, attempting to provide, and conspiring to provide material support or resources to a designated foreign terrorist organizations ("FTO")); (ii) Title 18, United States Code, Sections 2339D and 371 (receipt of, and attempting and conspiring to receive, military-type training from an FTO); (iii) Title 18, United States Code, Section 924 (firearms offenses related to crimes of violence); (iv) Title 50, United States Code, Section 1705 (making or receiving a contribution of funds, goods, and services to and from a specially designated terrorist); (v) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (vi) Title 18, United States Code,

Section 1425 (procurement of citizenship or naturalization unlawfully) (the “Subject Offenses”), including the following:

- Communications relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government;
- evidence of the identity(ies) of the user(s) of the Subject Accounts;
- evidence of the identities and locations of co-conspirators in the Subject Offenses, including photographs of and communications with such individuals;
- evidence of participation in the Subject Offenses by the user(s) of the Subject Accounts and others, including records relating to travel and financial transactions in furtherance of the Subject Offenses;
- evidence related to banks and other financial institutions at which the user(s) of the Subject Accounts conduct business, including, potentially, transactions in furtherance of the Subject Offenses;
- evidence of other online accounts the user(s) of the Subject Accounts, including potentially for operational activity or otherwise in furtherance of the Subject Offenses; and
- passwords or other information needed to access user’s computer or other online accounts.

1 MAG 4291

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with Three Email  
Accounts, Maintained at Premises  
Controlled by Google, Inc.

USAO Reference No. 2017R00116.

d)

SEARCH WARRANT

TO: Google, Inc. ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

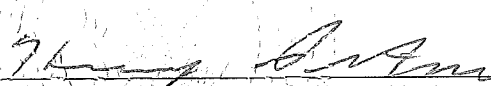
**1. Warrant.** Upon an affidavit of a Special Agent from the Investigative Agency, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the Google Accounts associated with the email addresses holy.smoke.shop.franklin@gmail.com, jacob.kouran@gmail.com, wmc.sportswear@gmail.com, which are maintained at premises controlled by Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

<u>6-6-17</u>	<u>5:02 PM</u>
Date Issued	Time Issued

<u></u>
HONORABLE HENRY B. PITMAN
United States Magistrate Judge
Southern District of New York



## **Email Search Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Google, Inc. (the “Provider”), headquartered in Mountain View, California, and applies to all content and other information within the Provider’s possession, custody, or control associated with the Google Accounts related to the email addresses holy.smoke.shop.franklin@gmail.com, jacob.kouran@gmail.com, wmc.sportswear@gmail.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Email Content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email);

b. *Search History.* All data concerning searches run by the user of the Subject Accounts, including, but not limited to, the content, date, and time of the search.

c. *Google+ Photos and Content.* All data concerning Google+ Photos, including all albums, photos, videos, and associated metadata for each file, as well as all Google+ posts, comments, profiles, contacts, and information relating to Google+ Circles.

d. *Google Drive Content.* All files and folders in the Google Drive associated with the Subject Accounts.

e. *Google Wallet Content.* All data and information in the Google Wallet associated with the Subject Accounts.

f. *YouTube Content.* For any YouTube account associated with the Subject Accounts, all subscriber information as well as copies of any videos and associated metadata and any YouTube comments or private messages.

g. *Android Content.* Any Android device information associated with the Subject Accounts, including IMEI/MEID, make and model, serial number, date and IP of last access to Google, and a list of all accounts that have ever been active on the device.

h. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

i. *Address Book Information.* All address book, contact list, or similar information associated with the Subject Accounts.

j. *Subscriber and Payment Information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

k. *Transactional Records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

l. *Customer Correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

m. *Location History.* Location data from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google related to the Subject Accounts.

n. *Preserved Records.* Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of (i) Title 18, United States Code, Section 2339B (providing, attempting to provide, and conspiring to provide material support or resources to a designated foreign terrorist organizations (“FTO”)); (ii) Title 18, United States Code, Sections 2339D and 371 (receipt of, and attempting and conspiring to receive, military-type training from an FTO); (iii) Title 18, United States Code, Section 924 (firearms offenses related to crimes of violence); (iv) Title 50, United States Code, Section 1705 (making or receiving a contribution of funds, goods, and services to and from a specially designated terrorist); (v) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (vi) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the “Subject Offenses”), including the following:

- Communications relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government;
- evidence of the identity(ies) of the user(s) of the Subject Accounts;
- evidence of the identities and locations of co-conspirators in the Subject Offenses, including photographs of and communications with such individuals;
- evidence of participation in the Subject Offenses by the user(s) of the Subject Accounts and others, including records relating to travel and financial transactions in furtherance of the Subject Offenses;
- evidence related to banks and other financial institutions at which the user(s) of the Subject Accounts conduct business, including, potentially, transactions in furtherance of the Subject Offenses;
- evidence of other online accounts the user(s) of the Subject Accounts, including potentially for operational activity or otherwise in furtherance of the Subject Offenses; and
- passwords or other information needed to access user's computer or other online accounts.

17 MAG 4291

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with Three Instagram  
Accounts, Maintained at Premises  
Controlled by Instagram LLC and  
Facebook, Inc.

B)

**SEARCH WARRANT**

TO: Instagram LLC and Facebook, Inc. (collectively, the "Provider")

Federal Bureau of Investigation (the "Investigative Agency")

1. **Warrant.** Upon an Affidavit of a federal law enforcement officer in connection with an investigation being conducted by the Investigative Agency, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the Instagram accounts associated with the email addresses ali.m.kourani@gmail.com, alikuku@hotmail.com, jacob.kouran@gmail.com (the "Subject Accounts"), which are maintained at premises controlled by the Provider, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Search Warrant, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Search Warrant on the Provider within 14 days of the date of issuance. The Search Warrant may

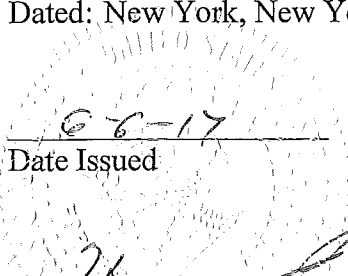
be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

06-17  
Date Issued

5:02 PM  
Time Issued

  
Henry B. Pitman  
HONORABLE HENRY B. PITMAN  
United States Magistrate Judge  
Southern District of New York

## **Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Instagram LLC and Facebook, Inc. (collectively, the “Provider”) and applies to all content and other information within the Provider’s possession, custody, or control associated with the Instagram accounts associated with the email addresses ali.m.kourani@gmail.com, alikuku@hotmail.com, jacob.kouran@gmail.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, which is not to be transmitted to the Provider.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

- a. Any “posts,” photographs, images, or videos and associated metadata associated with the Subject Account, including any galleries of photographs, images, or videos shared by the Subject Accounts, even if those photographs, images, or videos were uploaded from another service;
- b. All geolocation information for all photographs uploaded by the Subject Accounts;
- c. Any stored electronic messages and other stored content information, including all associated metadata, presently maintained in, or on behalf of, the Subject Accounts, and all



existing printouts from original storage of messages associated with the Subject Accounts, including all header information associated with such messages;

d. Any personal profile page information and any associated metadata, including but not limited to full name, user identification number, birth date, contact email addresses, physical addresses (including city, state, and zip code), telephone numbers, screen names, websites, and other personal information for the user;

e. Any lists of other users who are “following” or who are “followed” by the Subject Accounts, any groups of users or “lists” that the Subject Account follow or are followed by, and any recommendations of users to follow;

f. All communications and messages made or received by the Subject Accounts, including all accepted, rejected and pending “Follow” requests;

g. All transactional information concerning activity associated with the Subject Accounts, including Internet protocol address logs, cookie data, and all associated metadata;

h. All business records and subscriber information, in any form kept, concerning the Subject Accounts, including applications, account creation date and time, all full names, screen names, and account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records;

i. All records indicating the services available to subscribers of the Subject Accounts;

j. All privacy settings and other account settings, including any currently valid or previously used passwords, secret question/answers, or other login information associated with the Subject Accounts; and

k. All records pertaining to communications between the Provider and any person regarding the Subject Account, including contacts with support services and records of actions taken.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of (i) Title 18, United States Code, Section 2339B (providing, attempting to provide, and conspiring to provide material support or resources to a designated foreign terrorist organizations (“FTO”)); (ii) Title 18, United States Code, Sections 2339D and 371 (receipt of, and attempting and conspiring to receive, military-type training from an FTO); (iii) Title 18, United States Code, Section 924 (firearms offenses related to crimes of violence); (iv) Title 50, United States Code, Section 1705 (making or receiving a contribution of funds, goods, and services to and from a specially designated terrorist); (v) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (vi) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the “Subject Offenses”), including the following:

- Communications relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the

use and acquisition of weapons, and the making of false statements to the U.S. government;

- evidence of the identity(ies) of the user(s) of the Subject Accounts;
- evidence of the identities and locations of co-conspirators in the Subject Offenses, including photographs of and communications with such individuals;
- evidence of participation in the Subject Offenses by the user(s) of the Subject Accounts and others, including records relating to travel and financial transactions in furtherance of the Subject Offenses;
- evidence related to banks and other financial institutions at which the user(s) of the Subject Accounts conduct business, including, potentially, transactions in furtherance of the Subject Offenses;
- evidence of other online accounts the user(s) of the Subject Accounts, including potentially for operational activity or otherwise in furtherance of the Subject Offenses; and
- passwords or other information needed to access user's computer or other online accounts.

17 MAG 4291  
UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All  
Content and Other Information  
Associated with the Email Account  
jacobfashion@hotmail.com,  
Maintained at Premises Controlled by  
Microsoft Corporation.

USAO Reference No. 2017R00116.

SEARCH WARRANT

TO: Microsoft Corporation ("Provider")

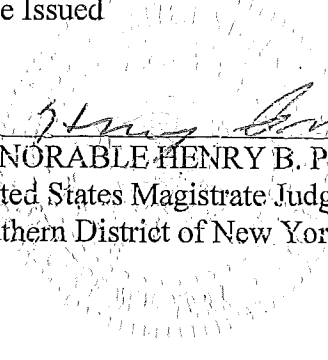
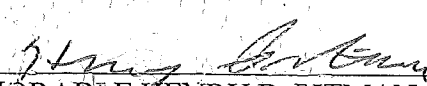
Federal Bureau of Investigation ("Investigative Agency")

**1. Warrant.** Upon an affidavit of a Special Agent from the Investigative Agency, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the email account jacobfashion@hotmail.com, maintained at premises controlled by Provider, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 30 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

<u>6-6-17</u>	<u>5:02 PM</u>
Date Issued	Time Issued

  
  
HONORABLE HENRY B. PITMAN  
United States Magistrate Judge  
Southern District of New York

## **Email Search Attachment A**

### **I. Subject Account and Execution of Warrant**

This warrant is directed to Microsoft Corporation (the “Provider”), headquartered at Redmond, Washington, and applies to all content and other information within the Provider’s possession, custody, or control associated with the email account jacobfashion@hotmail.com (the “Subject Account”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email Content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email);

b. *Address Book Information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and Payment Information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

- Communications relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government
- evidence of the identity(ies) of the user(s) of the Subject Account;
- evidence of the identities and locations of co-conspirators in the Subject Offenses, including photographs of and communications with such individuals;
- evidence of participation in the Subject Offenses by the user(s) of the Subject Account and others, including records relating to travel and financial transactions in furtherance of the Subject Offenses;
- evidence related to banks and other financial institutions at which the user(s) of the Subject Account conduct business, including, potentially, transactions in furtherance of the Subject Offenses;
- evidence of other online accounts the user(s) of the Subject Account, including potentially for operational activity or otherwise in furtherance of the Subject Offenses; and
- passwords or other information needed to access user's computer or other online accounts.



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

17 MAG 4291

In the Matter of Warrants for All  
Content and Other Information  
Associated With Two Twitter  
Accounts, Maintained at Premises  
Controlled by Twitter, Inc.

a)

**SEARCH WARRANT**

TO: Twitter, Inc. ("Provider")


Federal Bureau of Investigation ("Investigative Agency")

1. **Warrant.** Upon an Affidavit of a federal law enforcement officer in connection with an investigation being conducted by the Investigative Agency, pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe that the Twitter accounts associated with the email addresses ali.m.kourani@gmail.com and alikuku@hotmail.com (the "Subject Accounts"), which are maintained at premises controlled by the Provider, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 10 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order on the Provider within 14 days of the date of issuance. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

Dated: New York, New York

6-6-17                      5:02 PM  
Date Issued                      Time Issued

  
\_\_\_\_\_  
HONORABLE HENRY B. PITMAN  
United States Magistrate Judge  
Southern District of New York

## **Search Warrant Attachment A**

### **I. Subject Accounts and Execution of Warrant**

This warrant is directed to Twitter, Inc. (the “Provider”), with offices in San Francisco, California, and applies to all content and other information within the Provider’s possession, custody, or control associated with the Twitter accounts associated with the email addresses ali.m.kourani@gmail.com and alikuku@hotmail.com (the “Subject Accounts”).

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, which is not to be transmitted to the Provider.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts:

a. *Profile Information.* Any personal profile page information, including but not limited to biographical entries, photographs, and location information for the user of the Subject Accounts.

b. *Tweet Information.* Any tweets and related information, including any “favorite” or “retweet” information, any “mentions,” any lists in the “Connect” tab of other users who have responded to any tweets from the Subject Account, and “Tweet With Location” information.

c. *Photographs/Images.* Any photographs or images associated with each Subject Account, including any galleries of photographs or images shared by the Subject Account, even if those photographs or images were uploaded from another service.

d. *Link Information.* Any websites to which the Subject Accounts have linked, as well as any information concerning how often those links have been clicked.

e. *Associated Users.* Any lists of other users who are “following” or who are “followed” by each Subject Account, any groups of users or “lists” that the Subject Accounts follow or are followed by, and any recommendations of users to follow, such as any “Who To Follow” lists.

f. *Direct Messages.* Any direct messages sent to or by the Subject Accounts, and any related information.

g. *Subscriber and Billing Information.* Any records (1) showing identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses; (2) concerning the date on which the account was created, the IP address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services used by the subscriber; and (3) reflecting the subscriber’s means and source of payment, including any credit card or bank account number.

h. *Search Information.* Any records concerning searches performed by the Subject Accounts.

i. *Third-party Information.* Any records reflecting third-party websites with which the Subject Accounts are connected.

j. *Transactional Information.* Any records of transactional information about the use of the Subject Accounts on its system, including records of login (i.e., session) times and durations and the methods used to connect to the account (such as logging into the account through the Provider’s website).

k. *Customer Correspondence*. Any records of any customer-service contacts with or about the subscribers, including any inquiries or complaints concerning the subscriber's account(s).

l. *Preserved Records*. Any preserved copies of the foregoing categories of records with respect to the Subject Accounts.

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of (i) Title 18, United States Code, Section 2339B (providing, attempting to provide, and conspiring to provide material support or resources to a designated foreign terrorist organizations ("FTO")); (ii) Title 18, United States Code, Sections 2339D and 371 (receipt of, and attempting and conspiring to receive, military-type training from an FTO); (iii) Title 18, United States Code, Section 924 (firearms offenses related to crimes of violence); (iv) Title 50, United States Code, Section 1705 (making or receiving a contribution of funds, goods, and services to and from a specially designated terrorist); (v) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (vi) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the "Subject Offenses"), including the following:

- Communications relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from

Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government;

- evidence of the identity(ies) of the user(s) of the Subject Accounts;
- evidence of the identities and locations of co-conspirators in the Subject Offenses, including photographs of and communications with such individuals;
- evidence of participation in the Subject Offenses by the user(s) of the Subject Accounts and others, including records relating to travel and financial transactions in furtherance of the Subject Offenses;
- evidence related to banks and other financial institutions at which the user(s) of the Subject Accounts conduct business, including, potentially, transactions in furtherance of the Subject Offenses;
- evidence of other online accounts the user(s) of the Subject Accounts, including potentially for operational activity or otherwise in furtherance of the Subject Offenses; and
- passwords or other information needed to access user's computer or other online accounts.